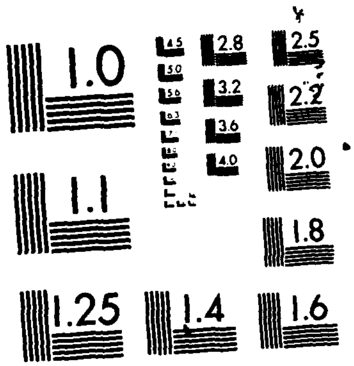
AD-A172 772 THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION(U) WISCONSIN UNIV-MADISON MATHEMATICS RESEARCH CENTER I J SCHOENBERG AUG 86 MRC-TSR-2954 1/1

UNCLASSIFIED DAAG29-80-C-0041 F/G 12/1 NL



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

3

MRC Technical Summary Report #2954

THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION

Isaac J. Schoenberg

Mathematics Research Center
University of Wisconsin—Madison
610 Walnut Street
Madison, Wisconsin 53705

August 1986

(Received August 13, 1986)

Sponsored by

U. S. Army Research Office
P. O. Box 12211
Research Triangle Park
North Carolina 27709

UNIVERSITY OF WISCONSIN-MADISON
MATHEMATICS RESEARCH CENTER

THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION

Isaac J. Schoenberg

Technical Summary Report #2954
August 1986

ABSTRACT

The Chinese Remainder Theorem is as follows: Given integers a_i $(i = 1,2,\ldots,n)$ and corresponding moduli m_i, which are pairwise relatively prime, than the n congruences

$$x \equiv a_i \bmod m_i \quad (i = 1,\ldots,n) \tag{1}$$

have a unique solution $x \bmod m$, where $m = m_1 m_2 \cdots m_n$.

Sometimes in the 1950s the late Hungarian-Swedish mathematician Marcel Riesz visited the University of Pennsylvania and told us informally that the above theorem is an analogue of the unique interpolation at n distinct data by a polynomial of degree $n - 1$.

It follows that (1) can be solved in two different ways:

1. By an analogue of Lagrange's interpolation formula.
2. By an analogue of Newton's solution by divided differences.

This analogy gives sufficient insight to furnish a proof of the theorem that $\varphi(m_1 m_2 \cdots m_n) = \varphi(m_1)\varphi(m_2)\cdots\varphi(m_n)$, where $\varphi(m)$ is Euler's function.

AMS (MOS) Subject Classifications: 10A10, 41A10

Key Words: Chinese Remainder Theorem, Polynomial Interpolation

Work Unit Number 3 (Numerical Analysis and Scientific Computing)

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

SIGNIFICANCE AND EXPLANATION

The Chinese Remainder Theorem is one of the most important results of elementary Number Theory as it was used by Kurt Gödel in one of his most fundamental papers in Logic. The paper uses the analogy with the theorem of polynomial interpolation to solve it in two different ways.

The responsibility for the wording and views expressed in this descriptive summary lies with MRC, and not with the author of this report.

THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION

Isaac J. Schoenberg

For given integers a_i $(1 \leq i \leq n)$ and positive integers m_i $(1 \leq i \leq n)$ that are pairwise relatively prime, the Chinese Remainder Problem (abbreviated to C.R.P.) may be stated as follows:

The Problem. To find an integer x satisfying the congruences

$$x \equiv a_i \pmod{m_i}, \quad (i = 1,2,\ldots,n) . \tag{1}$$

If we have found one solution x then clearly all solutions of (1) belong to a residue class modulo $M = m_1m_2\cdots m_n$.

Sometimes in the 1950's the late Hungarian-Swedish mathematician Marcel Riesz visited the University of Pennsylvania and told us informally that the C.R.P. (1) can be thought of as an analogue of the interpolation by polynomials: Given real values y_i $(1 \leq i \leq n)$ and distinct real values x_i, to find a polynomial $P(x)$ of degree $\leq n - 1$ such that

$$P(x_i) = y_i, \quad (i = 1,2,\ldots,n) . \tag{2}$$

We can solve (2) by Lagrange's formula

$$P(x) = \sum_1^n y_i L_i(x) , \tag{3}$$

where the fundamental functions

$$L_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

Sponsored by the United States Army under Contract No. DAAG29-80-C-0041.

are such that they satisfy the equations

$$L_i(x_j) = \delta_{ij}, \quad (i,j = 1,\ldots,n) . \tag{4}$$

Here the δ_{ij}, called the Kronecker deltas, are defined by

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j , \\ 0 & \text{if } i \neq j . \end{cases} \tag{5}$$

To solve the C.R.P. suppose that we proceed similarly, letting the integers a_i be the analogues of the y_i, and defining integers b_i such that

$$b_i \equiv \delta_{ij} \pmod{m_j}, \quad (i,j = 1,\ldots,n) , \tag{6}$$

as the analogues of the functions $L_i(x)$. This leads to

Theorem 1. <u>A solution of the system</u> (1) <u>is given by</u>

$$x = \sum_1^n a_i b_i . \tag{7}$$

Indeed, as the b_i satisfy (6), we find from (7) that

$$x = \sum_1^n a_i b_i \equiv \sum_{i=1}^n a_i \delta_{ij} \equiv a_j \pmod{m_j} \quad \text{for all} \quad j = 1,\ldots,n .$$

Example 1. To find x satisfying

$$x \equiv 2 \pmod 5, \; x \equiv 6 \pmod 7, \; x \equiv 5 \pmod{11} . \tag{8}$$

We are to solve (6) which in our case is

$$\begin{aligned} &b_1 \equiv 1 \pmod 5, && b_1 \equiv 0 \pmod 7, && b_1 \equiv 0 \pmod{11} , \\ &b_2 \equiv 0 \pmod 5, && b_2 \equiv 1 \pmod 7, && b_2 \equiv 0 \pmod{11} , \\ &b_3 \equiv 0 \pmod 5, && b_3 \equiv 0 \pmod 7, && b_3 \equiv 1 \pmod{11} , \end{aligned}$$

from which we obtain that

$$b_1 \equiv 231, \quad b_2 \equiv 330, \quad b_3 \equiv 210 .$$

By (7) we find that all solutions of (8) are given by

$$x \equiv 27 \pmod{385}, \quad \text{where} \quad 385 = 5 \cdot 7 \cdot 11 .$$

The solution (7) of the C.R.P. (1) is essentially the solution as given by G. E. Andrews in [1], and by E. Grosswald in [2], without mentioning the analogy with Lagrange's formula. My colleague Richard Askey tells me that Riesz' remark is well known to computer scientists, but apparently not to mathematicians.

Besides recording Riesz' remark, the author's contribution is the following remark: Newton solves the interpolation problem (2) using successive divided differences c_i to obtain

$$P(x) = c_1 + c_2(x - x_1) + c_3(x - x_1)(x - x_2) + \cdots + c_n(x - x_1)(x - x_2) \ldots (x - x_{n-1}) , \tag{9}$$

where the coefficients c_i are obtained by solving

$$\begin{aligned} y_1 &= c_1 \\ y_2 &= c_1 + c_2(x_2 - x_1) \\ &\vdots \\ y_n &= c_1 + c_2(x_n - x_1) + c_3(x_n - x_1)(x_n - x_2) \\ &\quad + \cdots + c_n(x_n - x_1)(x_n - x_2) \ldots (x_n - x_{n-1}) . \end{aligned} \tag{10}$$

Applying Newton's idea to the solution of the C.R.P. (1), we consider the m_i to be the analogues of the $x - x_i$ and seek to determine the integer d_i $(1 \leq i \leq n)$ from the system of congruences

$$\begin{aligned} d_1 &\equiv a_1 \pmod{m_1} \\ d_1 + d_2 m_1 &\equiv a_2 \pmod{m_2} \\ d_1 + d_2 m_1 + d_3 m_1 m_2 &\equiv a_3 \pmod{m_3} \\ &\vdots \\ d_1 + d_2 m_1 + d_3 m_1 m_2 + \cdots + d_n m_1 m_2 \ldots m_{n-1} &\equiv a_n \pmod{m_n} . \end{aligned} \tag{11}$$

In this way we obtain

Theorem 2. A solution of the C.R.P. (1) is obtained as follows: We first determine the integers d_i as solutions of the congruences (11), and then a solution of (1) is given by

$$x = d_1 + d_2m_1 + d_3m_1m_2 + \cdots + d_nm_1m_2 \cdots m_{n-1} \ . \qquad (12)$$

Indeed, notice that by (11), the x given by (12), satisfies all congruences (1): For any k, $1 \leq k \leq n$, from (12) we get that

$$x \equiv d_1 + d_2m_1 + \cdots + d_km_1m_2 \cdots m_{k-1} \pmod{m_x}$$

and therefore, by the k-th congruence (11), we have that $x \equiv a_k \pmod{m_k}$.

Example 2. Let us solve the C.R.P. (8) by the Newton approach. For (8) we have $n = 3$, $a_1 = 2$, $a_2 = 6$, $a_3 = 5$, $m_1 = 5$, $m_2 = 7$, $m_3 = 11$. As we can always choose $d_1 = a_1 = 2$, the remaining $n - 1 = 2$ congruence (11) are

$$2 + 5d_2 \equiv 6 \pmod{7} \ ,$$

$$2 + 5d_2 + 35d_3 \equiv 5 \pmod{11} \ .$$

The first has the solution $d_2 = 5$ and the second now becomes $2 + 25 + 35d_3 \equiv 5 \pmod{11}$ whose solution is $d_3 = 0 \pmod{11}$. From (12), for $n = 3$ we obtain that $x = 27$ is a solution of (8).

A consequence of Theorem 1, or of Theorem 2, is the following

Corollary 1. The Chinese Remainder Problem (1) has always a unique solution x, mod M, where $M = m_1m_2 \ldots m_n$.

Moreover, either of the theorems gives a method of finding this unique solution.

Let us keep fixed the n pairwise relatively prime moduli $m_1, m_2, \ldots, m_n$. How many Chinese Residue Problems (1) correspond to them? Evidently their number is M for we may restrict the a_i to assume the values of a residue system mod m_i, for instance

$$a_i = 0, 1, \ldots, m_i - 1, \quad (i = 1, \ldots, n) \ . \qquad (13)$$

For every choice of the n-tuple $(a_1, a_2, \ldots, a_n)$ there corresponds a unique solution x of (1) which assumes one of the values

$$x \in \{0,1,\ldots,M-1\} \quad (M = m_1,\ldots,m_n) \ . \tag{14}$$

Corollary 2. <u>There is a one-to-one correspondence between the n-tuples</u> $(a_1,\ldots,a_n)$, <u>subject to</u> (13), <u>and the</u> M <u>possible values</u> (14) <u>of</u> x.

For if two distinct n-tuples

$$(a_1,a_2,\ldots,a_n) \neq (a_1',a_2',\ldots,a_n') \tag{15}$$

lead to equal x's: $x = x'$ we would get from (1) that

$$a_i \equiv a_i' \pmod{m_i}, \quad (i = 1,\ldots,n) \ ,$$

in contradiction to our assumption (15).

Example 3. We choose the simplest possible example: Let $n = 2$, $m_1 = 2$, $m_2 = 3$, hence $M = 6$. Here, by (13) we may choose $a_1 = 0,1$ and $a_2 = 0,1,2$. Denoting by x_r the solutions of the 6 C.R.Ps. we find these C.R.Ps to be

$$\begin{array}{llll} \text{(a)} & x_1 \equiv 0 \pmod 2 & \text{(b)} \ x_2 \equiv 0 \pmod 2 & \text{(c)} \ x_3 \equiv 0 \pmod 2 \\ & x_1 \equiv 0 \pmod 3 & \ x_2 \equiv 1 \pmod 3 & \ x_3 \equiv 2 \pmod 3 \\ \text{(d)} & x_4 \equiv 1 \pmod 2 & \text{(e)} \ x_5 \equiv 1 \pmod 2 & \text{(f)} \ x_6 \equiv 1 \pmod 2 \\ & x_4 \equiv 0 \pmod 3 & \ x_5 \equiv 1 \pmod 3 & \ x_6 \equiv 2 \pmod 3 \ . \end{array} \tag{16}$$

Their solutions are easily found to be

$$x_1 = 0, \ x_2 = 4, \ x_3 = 2, \ x_4 = 3, \ x_5 = 1, \ x_6 = 5 \ , \tag{17}$$

which indeed form a residue system modulo $M = 6$.

We wish to close our note with an elementary application of the one-to-one mapping expressed by Corollary 2. For this we need

Corollary 3. <u>In the Chinese Remainder Problem</u> (1) <u>we have</u>

$$(a_i,m_i) = 1 \quad \text{for all} \quad i = 1,\ldots,n \tag{18}$$

<u>if and only if for the solution</u> x <u>of</u> (1) <u>we have</u>

$$(x,m_1m_2\ldots m_n) = 1 \ . \tag{19}$$

Indeed, by (1) we see that (18) holds iff $(x,m_i) = 1$ for all i, which is equivalent to (19).

As usual we denote by $\varphi(m)$ the Euler function giving the number of positive numbers $\leq m$ which are relatively prime to m. The application we had in mind is

Corollary 4. For the pairwise relatively prime m_i we have

$$\varphi(m_1 m_2 \cdots m_n) = \varphi(m_1)\varphi(m_2) \cdots \varphi(m_n) . \tag{20}$$

Because the left side is = number of solutions x of (1) satisfying (19), while the right side gives the number of C.R.Ps. (1) satisfying the conditions (18).

Example 4. For the moduli $m_1 = 2$ and $m_2 = 3$ of Example 3 only two C.R.Ps. (e) and (f) satisfy the conditions (18). Also notice that their solutions $x_5 = 1$ and $x_6 = 5$ indeed form a reduced residue system mod 6 as they should.

Remarks. 1. The second Newton approach is slightly more economical then the first approach: while the first requires to determine the n integers b_i $(i = 1,2,\ldots,n)$, the Newton approach requires only to find the $n - 1$ integers d_i $(i = 2,3,\ldots,n)$.

2. I owe to Gerald Goodman the reference [3] in which Ulrich Oberst shows that appropriate abstract formulations of the Chinese Remainder Problem can be made the basis of much of Modern Algebra including the main theorems of Galois theory.

3. My colleague Stephen C. Kleene informs me that Kurt Gödel uses the solution of the Chinese Remainder Problem (without its name) in his fundamental paper "On formally undecidable propositions of Principia Mathematica and related systems 1" in [4], 145-195, especially Lemma 1 on page 135. See also Footnote i on page 136.

4. Originally I wrote this note very briefly, even tersely. I owe to the Editor an expanded version of this note which I found very helpful in casting it in the present form.

5. In a sequel to the present paper it will be shown how to apply the Chinese Remainder theorem to obtain indices for moduli which do not admit primitive roots. These indices will be vectors.

REFERENCES

1. G. E. Andrews, Number Theory, W. B. Saunders Co., Philadelphia, 1971.

2. Emil Grosswald, Topics from the Theory of Numbers, The Macmillan Co., New York, 1966.

3. Ulrich Oberst, Anwendungen des chinesischen Restsatzes, Expositiones Mathematicae, vol. 3 (1985), 97-148.

4. Kurt Gödel, Collected Works, volume 1, Oxford University Press, New York, 1986.

5. I. J. Schoenberg, On the theory and practice of indices mod m, to appear.

IJS:scr

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 2954	2. GOVT ACCESSION NO. AD-A172772	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) THE CHINESE REMAINDER PROBLEM AND POLYNOMIAL INTERPOLATION		5. TYPE OF REPORT & PERIOD COVERED Summary Report - no specific reporting period
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Isaac J. Schoenberg		8. CONTRACT OR GRANT NUMBER(s) DAAG29-80-C-0041
9. PERFORMING ORGANIZATION NAME AND ADDRESS Mathematics Research Center, University of Wisconsin 610 Walnut Street Madison, Wisconsin 53705		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Work Unit Number 3 - Numerical Analysis and Scientific Computing
11. CONTROLLING OFFICE NAME AND ADDRESS U. S. Army Research Office P.O. Box 12211 Research Triangle Park, North Carolina 27709		12. REPORT DATE August 1986
		13. NUMBER OF PAGES 8
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Chinese Remainder Theorem
Polynomial Interpolation

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Chinese Remainder Theorem is as follows: Given integers a_i $(i = 1,2,\ldots,n)$ and corresponding moduli m_i, which are pairwise relatively prime, than the n congruences

$$x \equiv a_i \bmod m_i \quad (i = 1,\ldots,n) \tag{1}$$

have a unique solution $x \bmod m$, where $m = m_1 m_2 \ldots m_n$.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

20. ABSTRACT - cont'd.

Sometimes in the 1950s the late Hungarian-Swedish mathematician Marcel Riesz visited the University of Pennsylvania and told us informally that the above theorem is an analogue of the unique interpolation at n distinct data by a polynomial of degree $n - 1$.

It follows that (1) can be solved in two different ways:

1. By an analogue of Lagrange's interpolation formula.
2. By an analogue of Newton's solution by divided differences.

This analogy gives sufficient insight to furnish a proof of the theorem that $\varphi(m_1 m_2 \ldots m_n) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_n)$, where $\varphi(m)$ is Euler's function.

END
11-86
DTIC